# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

ABSTRACTED-PUB-NO: JP07202884A

BASIC-ABSTRACT:

The codec decodes the input individual information (152) using master key (Kmi). After decoding, the work key (kw) is stored. Another code decoder (103) uses this work key and carries out decoding of the input common information (151). A PN signal generator (107) uses the a scramble key (KS) and generates PN signal.

A descrambler (106) uses the PN signal and descrambler input data (150). A time information memory and timer (109), stores the updating time information included in the decoded individual information. The power supply (125) controlled by a power supply control unit (121) is switched ON, for execution of the above operations,

ADVANTAGE - Updates code key reliably simply, and efficiently.

CHOSEN-DRAWING: Dwg.3/4

TITLE-TERMS: CODEC TRANSCEIVER TRANSMIT INFORMATION DECODE FIRST CODEC UPDATE INFORMATION ENCIPHER SECOND DECODE

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平７－２０２８８４

(43)公開日　平成７年（１９９５）８月４日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|
| H04L 9/18 | | | | |
| H04H 1/00 | | F | | |
| | | | H04L 9/02 | B |

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平５－３３６０８８

(22)出願日　平成５年（１９９３）１２月２８日

(71)出願人　０００００２１８５
ソニー株式会社
東京都品川区北品川６丁目７番３５号

(72)発明者　板倉　英三郎
東京都品川区北品川６丁目７番３５号　ソニー　株式会社内

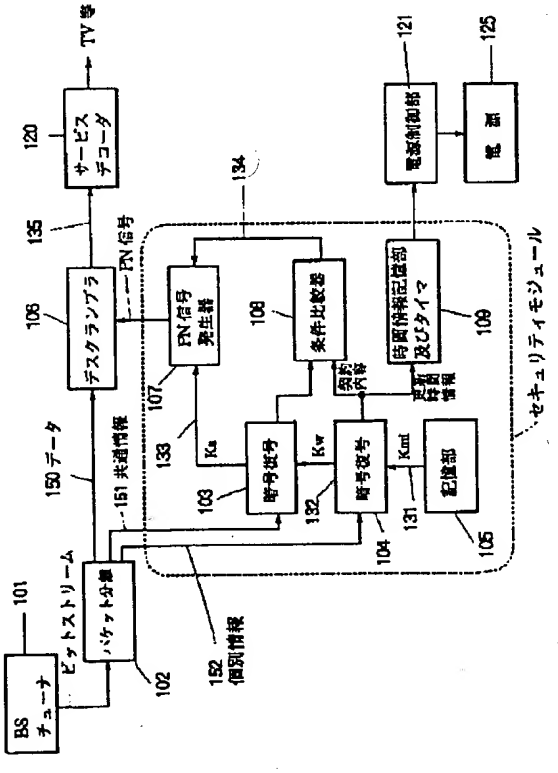
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】送信装置および受信装置

(57)【要約】

【目的】　簡単かつ確実に有料放送の暗号鍵を効率的に更新する。

【構成】　暗号復号器１０４は、入力される個別情報１５２を、マスタ鍵Kmiを用いて復号し、その中に含まれるワーク鍵ＫＷを記憶する。暗号復号器１０３は、入力される共通情報１５１を、ワーク鍵ＫＷを用いて復号する。ＰＮ信号発生器１０７は、スクランブル鍵ＫＳを用いてＰＮ信号を生成する。デスクランブラ１０５は、入力されるデータ１５０をＰＮ信号を用いてデスクランブルする。暗号復号器１０４により復号された個別情報に含まれる更新時間情報が時間情報記憶部及びタイマ１０９に記憶され、この記憶した時刻になったとき、電源１２５がオンされる。



1

【特許請求の範囲】

【請求項１】　伝送すべき情報を発生する第１の発生手段と、

前記情報を暗号化する暗号鍵と、前記暗号鍵を更新する更新情報を発生する第２の発生手段と、

前記第２の発生手段により発生された前記暗号鍵に対応して、前記第１の発生手段が発生する情報を暗号化する第１の暗号化手段と、

前記暗号鍵と更新情報を暗号化する第２の暗号化手段と、

前記第１の暗号化手段により暗号化された情報、並びに前記第２の暗号化手段により暗号化された前記暗号鍵と更新情報を伝送する伝送手段とを備えることを特徴とする送信装置。

【請求項２】　所定のタイミングで更新される暗号鍵を用いて、伝送された情報、前記暗号鍵、および前記暗号鍵の更新情報を受信する受信装置において、

前記更新情報を記憶する第１の記憶手段と、

前記第１の記憶手段に記憶された前記更新情報に基づき、電源を制御する制御手段と前記更新情報手段に基づいて更新される前記暗号鍵を記憶する第２の記憶手段と、

前記第２の記憶手段に記憶された前記記憶鍵に基づいて前記情報を復号する復号手段とを備えたことを特徴とする受信装置。

【請求項３】　前記更新情報は、前記暗号鍵を更新する更新開始時刻を含み、

前記制御手段は、前記更新開始時刻に、前記電源を一定時間オンすることを特徴とする請求項２に記載の受信装置。

【請求項４】　前記更新情報は、前記暗号鍵を更新する更新開始時刻及び前記暗号鍵の更新期間を含み、

前記制御手段は、前記更新開始時刻に前記電源をオンさせるとともに、前記更新期間に対応する時間経過後に前記電源をオフさせることを特徴とする請求項２に記載の受信装置。

【請求項５】　前記更新情報は、前記暗号鍵を更新する更新開始時刻及び前記暗号鍵の更新終了時刻を含み、

前記制御手段は、前記更新開始時刻に前記電源をオンさせるとともに、前記更新終了時刻に前記電源をオフさせることを特徴とする請求項２に記載の受信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、例えば有料放送において使用されるワーク鍵を自動更新する有料放送送受信装置に用いて好適な送信装置および受信装置に関する。

【０００２】

【従来の技術】従来より、有料放送で用いられる暗号は、通常階層構造になっており、複数の鍵を利用して暗号化している。さらにこの鍵が、試行錯誤的に検査して

2

順次発見されないように、送信側で周期的に鍵の更新が行われている。

【０００３】従来の有料衛星放送方式における鍵の階層構成を、図４を用いて説明する。図４に示すように、従来の階層構成の鍵は、３重の鍵（スクランブル鍵ＫＳ、ワーク鍵ＫＷ、マスター鍵Ｋｍｉ）で構成されている。まず、エンコーダである送出装置２１０側では、図示しないデータ送出器からのデータを、スクランブラ２０１で共通情報であるスクランブル鍵ＫＳによりスクランブルして送出し、デコーダである受信装置２２０側でデスクランブラ２０５によりデスクランブルする。このとき、後述するように、受信契約が有効な場合においてのみデスクランブルができるようになっている。

【０００４】スクランブラ２０１に入力されるスクランブル鍵ＫＳは、非常に短い周期（たとえば１秒）で更新されており、解読されないように、比較的更新周期の長いワーク鍵ＫＷを用いて暗号器２０２で暗号化され、受信装置２２０に送信される。ここで、送出装置２１０は、契約者に届けられたデコーダである受信装置２２０毎に付けられた個有のＩＤと、それに対応したマスター鍵Ｋｍｉを記憶部２０４にあらかじめ記憶している。そして各個人に割り当てられるワーク鍵ＫＷは、各デコーダ個有のマスター鍵Ｋｍｉを用いて暗号器２０３で暗号化され受信装置２２０に送信される。

【０００５】デコーダである受信装置２２０では、この個別に送信された暗号器２０３の出力である個別情報内のワーク鍵ＫＷを、記憶部２０８に記憶されている各デコーダ個有のマスター鍵Ｋｍｉを用いて暗号復号器２０７でデコードし、記憶する。そして、記憶されたワーク鍵ＫＷで、暗号器２０２の出力である共通情報内のスクランブル鍵ＫＳをデコードし、記憶する。記憶したスクランブル鍵ＫＳで、スクランブラ２０１からの出力情報をデスクランブラ２０５でデスクランブルする。このように、受信契約が有効な場合（マスタ鍵Ｋｍｉ、ワーク鍵ＫＷ、およびスクランブル鍵ＫＳが、正しいものである場合）にだけ、受信（デスクランブル）ができるようになっている。そして、復号されたデータは図示しないサービスデコーダへ出力される。

【０００６】各人個有のワーク鍵ＫＷをデコーダ個有のマスター鍵Ｋｍｉで暗号化して、所定のタイミングで送信（更新）する場合、更新周期の間に次のワーク鍵を配送すれば良いわけだが、更新周期の長さを大きく取ることで、加入者の個別情報をその分だけ多く送信できるため、加入者の数も多くできる。そこで現在、例えばＪＳＢ（日本衛星放送）では、ワーク鍵ＫＷの更新周期は１年とされている。その更新時にはデコーダが電源オンの状態、すなわちＪＳＢを視聴している必要があるため、現在ではダイレクトメールや告知放送という形で更新時を知らせ、加入者に電源をオンさせるようになっている。また一回の伝送で視聴者がワーク鍵を受け取ること

ができるとは限らないために、何度か送るようにしており、それでも更新されない場合、または、クレームがきたとき、は個々に送信するなどの手段で対処している。

【０００７】

【発明が解決しようとする課題】しかしながら、上述したように、従来のワーク鍵の更新方法は、ダイレクトメールや告知放送など人手を介して行う必要があり、加入者が増加すればするほど、手続きや管理は繁雑になるという問題がある。また、加入者にデコーダの電源をオンにすることを任せているために、当然ながら電源をオンせずにワーク鍵が更新されないような事が生じる虞がある。実際、例えば現行のＢＳ有料放送においては約１％のデコーダが更新不可となっている。

【０００８】さらに、現在はサービス（有料番組）の数が少ないためトラブルも少ないが、今後衛星データ放送等で多くのサービスが提供されると、それぞれのサービスにワーク鍵が必要で、その更新のためのトラブルも増加するものと考えられる。さらにまた、加入者がワーク鍵を確実に更新させるために、装置の電源スイッチをオンし続ける可能性があり、無駄な電力消費をする虞もある。

【０００９】本発明は上記事情に鑑みてなされたものであり、簡単かつ確実に暗号鍵を効率的に更新できる送信装置受信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明の送信装置は、伝送すべき情報としてのスクランブル鍵ＫＳを含む共通情報を発生する第１の発生手段としての共通情報発生回路３と、スクランブル鍵ＫＳを暗号化する暗号鍵としてのワーク鍵ＫＷと、ワーク鍵ＫＷを更新する更新情報としての個別情報を発生する第２の発生手段としての個別情報発生回路５と、個別情報発生回路５により発生されたワーク鍵ＫＷに対応して、共通情報発生回路３が発生するスクランブル鍵ＫＳを暗号化する第１の暗号化手段としての暗号器６と、ワーク鍵ＫＷと更新情報を暗号化する第２の暗号化手段としての暗号器８と、暗号器６により暗号化されたスクランブル鍵ＫＳ、並びに暗号器８により暗号化されたワーク鍵ＫＷと更新情報を伝送する伝送手段としての送信回路９とを備えることを特徴とする。

【００１１】本発明の受信装置は、所定のタイミングで更新される暗号鍵としてのワーク鍵ＫＷを用いて、伝送された情報、ワーク鍵ＫＷ、およびワーク鍵ＫＷの更新情報を受信する受信装置において、更新情報を記憶する第１の記憶手段としての時間情報記憶部及びタイマ１０９と、時間情報記憶部及びタイマ１０９に記憶された更新情報に基づいて電源１２５を制御する制御手段としての電源制御部１２１と、更新情報に基づいて更新されるワーク鍵ＫＷを記憶する第２の記憶手段としての暗号器１０４と、暗号復号器１０４に記憶されたワーク鍵ＫＷに基づいて情報を復号する復号手段としての暗号復号器１０３とを備えることを特徴とする。



【００１２】更新情報が、ワーク鍵ＫＷを更新する更新開始時刻を含む場合、時間情報記憶部及びタイマ１０９は、更新開始時刻に、電源１２５を一定時間オンするようにすることができる。

【００１３】更新情報が、ワーク鍵ＫＷを更新する更新開始時刻及びワーク鍵ＫＷの更新期間を含む場合、時間情報記憶部及びタイマ１０９は、更新開始時刻に電源１２５をオンさせるとともに、更新期間に対応する時間経過後に、電源１２５をオフさせるようにすることができる。

【００１４】更新情報が、ワーク鍵ＫＷを更新する更新開始時刻及びワーク鍵ＫＷの更新終了時刻を含む場合、時間情報記憶部及びタイマ１０９は、更新開始時刻に電源１２５をオンさせるとともに、更新終了時刻に電源１２５をオフさせるようにすることができる。

【００１５】

【作用】上記構成の送信装置では、暗号器６により暗号化されたスクランブル鍵ＫＳ、並びに暗号器８により暗号化されたワーク鍵ＫＷと更新情報が、送信回路９により伝送路に伝送される。従って、無駄に電力を消費することなく、ワーク鍵ＫＷを確実に更新させることが可能になる。

【００１６】上記構成の受信装置では、暗号復号器１０４は、ワーク鍵ＫＷを更新毎に書き換えて記憶する。また、時間情報記憶部及びタイマ１０９は、更新情報を記憶する。時間情報記憶部及びタイマ１０９からの制御信号に基づいて電源制御部１２１が電源１２５を制御することで、簡単かつ確実に、ワーク鍵ＫＷを効率的に更新することを可能とする。

【００１７】

【実施例】図１乃至図３は、本発明の送信装置と受信装置を応用した有料放送送信装置と受信装置の一実施例に係わり、図１は有料放送送信装置であるエンコーダの一実施例の要部の構成を示すブロック図、図２は図１のエンコーダに用いられる個別情報の一構成例を説明する説明図、図３は有料放送受信装置であるデコーダの一実施例の要部構成を示すブロック図である。

【００１８】図１のエンコーダにおいては、データ供給装置１が出力する転送すべきデータ（例えば新聞、雑誌等のキャラクタデータ）がスクランブラ２に供給され、スクランブルされるようになされている。共通情報発生回路３が発生する共通情報に含まれる。スクランブル鍵ＫＳがＰＮ信号発生器４に供給され、ＰＮ信号発生器４が発生したＰＮ信号がスクランブル２に供給されている。共通情報発生回路３が出力するスクランブル鍵ＫＳと、それに対応する番組番号等を含む共通情報は、暗号器６に供給され、個別情報発生回路５が出力する個別情報の内、ワーク鍵ＫＷに対応して、暗号化されるようになされている。

5

【００１９】また、個別情報発生回路５が出力する個別情報（図２を参照してご述するように、契約内容、ワーク鍵ＫＷ、次回更新時間情報等を含む）は、暗号器８に供給され、マスタ鍵発生回路７が発生するマスタ鍵Ｋｍｉに対応して暗号化されるようになされている。

【００２０】送信回路９は、スクランブラ２、暗号器６ならびに暗号器８より供給されるデータを合成し、アンテナ１０を介して、例えば衛星に伝送するようになされている。

【００２１】図２は、個別情報発生回路５が出力する個別情報の例を表している。この個別情報は、同図に示すように、符号化識別情報１６１（１６ビット）、関連情報識別情報１６２（２ビット）、ユーザＩＤ１６３（３２ビット）、ワーク鍵（ＫＷ）１６４（３２ビット）、ワーク鍵対象番組情報１６５（ＰＶ，ＳＶ，ＰＲ：４０ビット）、契約登録コード１６６（１２ビット）、鍵有効期限情報１６７（１１ビット）、個別情報送信予定日時情報１６８（１０ビット）、改ざん検出情報１６９（１６ビット）、その他の情報１７０（５ビット）から構成されていて、電気技術審議会の答申に基づいている。

【００２２】このように、共通情報は、各受信者に共通の情報を含んでいるが、個別情報は、個々の受信者毎に異なる情報を含んでいる。

【００２３】次に、図１の実施例の動作について説明する。共通情報発生回路３が発生するスクランブル鍵ＫＳは、ＰＮ信号発生器４に供給される。ＰＮ信号発生器４は、入力されるスクランブル鍵ＫＳに対応してＰＮ信号を発生し、スクランブラ２に供給する。スクランブラ２は、データ供給装置１より供給されるデータを、ＰＮ信号発生器４より入力されるＰＮ信号に対応してスクランブルし、送信回路９に出力する。このスクランブル鍵ＫＳは、比較的短い周期（例えば１秒毎）で変更（更新）される。

【００２４】個別情報発生回路５が出力する個別情報のうち、ワーク鍵ＫＷは、暗号器６に供給されている。暗号器６は、このワーク鍵ＫＷに対応して、共通情報発生回路３より供給されるスクランブル鍵ＫＳを暗号化し、送信回路９に出力する。このスクランブル鍵ＫＳは、その更新周期（１秒間）の間に、少なくとも１回出力される。

【００２５】また、暗号器８には、マスタ鍵発生回路７が発生するマスタ鍵Ｋｍｉが入力されており、暗号器８は、このマスタ鍵Ｋｍｉに対応して、個別情報発生回路５より入力される個別情報を暗号化し、送信回路９に出力する。

【００２６】送信回路９は、スクランブラ２、暗号器６及び暗号器８より供給されるデータを合成し、アンテナ１０を介して衛星に電波で伝送する。

【００２７】このようにして、伝送された情報は、衛星を介して図３に示すデコーダに電波で送信される。

6

【００２８】本実施例のデコーダでは、図３に示すように、衛星より伝送された有料放送をＢＳチューナ１０１で受信する。ＢＳチューナ１０１から出力されたビットストリームはパケット分離回路１０２に入力され、それぞれ暗号化されたデータ１５０、共通情報１５１（番組番号、スクランブル鍵ＫＳ等）、個別情報１５２（契約内容、ワーク鍵ＫＷ、次回更新時間情報等）の３種類のパケットに分離される。尚、１０１はＢＳチューナに限らず、ＣＳチューナあるいはＣＡＴＶの端末でも良い。

【００２９】データ１５０はスクランブル鍵ＫＳによりスクランブルされたデータであり、共通情報１５１は、ワーク鍵ＫＷにより暗号化され、データ１５０の番組番号やスクランブル鍵ＫＳ等から構成されている。また、図２に示すような個別情報１５２は、マスタ鍵Ｋｍｉにより暗号化されている。

【００３０】分離された個別情報１５２（ワーク鍵（ＫＷ’）１６４を含む）は、記憶部１０５に予め記憶されている各デコーダ個有のマスタ鍵（Ｋｍｉ）１３１を用いて、暗号復号器１０４で復号され、そのうちのワーク鍵ＫＷはそこに記憶される。そして、記憶されたワーク鍵（ＫＷ）１３２が、暗号復号器１０３に入力され、これを用いて、暗号復号器１０３で、共通情報１５１（スクランブル信号ＫＳ’を含む）が復号され、そのうちのスクランブル鍵（ＫＳ）１３３が、ＰＮ信号発生器１０７に入力される。

【００３１】条件比較器１０８は、暗号復号器１０４より供給される個別情報１５２内の契約条件を記憶すると共に、記憶した契約条件と、暗号復号器１０３から入力される共通情報１５１の内容とを比較し、契約条件と共通情報１５１の内容とが適合した場合、ＰＮ信号発生器１０７にイネーブル信号１３４を出力する。ＰＮ信号発生器１０７は、イネーブル信号１３４が入力されているとき、暗号復号器１０３からのスクランブル鍵ＫＳ１３３を基にしてＰＮ信号を生成し、デスクランブラ１０６に出力する。

【００３２】そしてデスクランブラ１０６は、ＰＮ信号によりデータ１５０をデスクランブルして番組データ１３５を得て、サービスデコーダ１２０に出力する。サービスデコーダ１２０は番組データ１３５をデコードし、図示しないＴＶ、専用端末等に出力する。

【００３３】一方、暗号復号器１０４で復号された個別情報１５２内の更新情報としての個別情報送信予定日時情報１６８（次回の個部情報送信予定日時を表す）は、時間情報記憶部及びタイマ１０９に出力されており、時間情報記憶部及びタイマ１０９は、個別情報送信予定日時情報１６８を記憶し、タイマをセットする。この時間情報記憶部及びタイマ１０９は、記憶した次回の個別情報送信予定時刻になると、電源制御部１２１へ制御信号を出力し、電源制御部１２１はこの制御信号によりデコ

ータの電源１２５をオンする。従って、デコーダは、更新時に、確実に動作状態となり、個別情報１５２を受信し、ワーク鍵KWを更新し、暗号復号基０４に記憶する。

【００３４】尚、電源オンの期間は、個別情報の送信期間が予め予測可能であるので、一定時間（例えば１時間）とし、その期間にワーク鍵KWを更新し、暗号復号基１０４に記憶し、その後電源１２５をオフする。

【００３５】このように本実施例のデコーダによれば、時間情報記憶部及びタイマ１０９からの制御信号により電源制御部１２１が自動的に電源１２５をオンし、電源オンの状態で個別情報１５２を受信し、ワーク鍵KWを更新し、暗号復号器１０４に記憶するので、簡単かつ確実に有料放送の個別情報を効率的に更新できる。

【００３６】尚、電源オンの制御は、上記実施例の方法（一定時間オン）に限らず、個別情報１５２内のワーク鍵更新時間情報として、個別情報送信予定日時情報１６８に、ワーク鍵更新開始時刻とこのワーク鍵更新開始時刻から電源をオンさせる継続時間とを設定し、デコーダの時間情報記憶部及びタイマ１０９によりワーク鍵更新開始時刻に電源をオンして、継続時間経過後に電源をオフすることで、ワーク鍵KWを更新し、暗号復号器１０４に記憶するようにしても良い。

【００３７】この場合、上記効果に加え、個別情報に更新開始時刻と電源をオンさせる継続時間を設定することにより、加入者の増減やサービスの変化に伴う次回の個別情報送信時間のばらつきに柔軟に対処することができる。

【００３８】また、電源オンの制御のその他の方法として、個別情報１５２内のワーク鍵更新時間情報として、ワーク鍵更新開始時刻とワーク鍵更新終了時刻を設定し、この２つの情報からデコーダの時間情報記憶部及びタイマ１０９により電源をオン／オフさせるようにしても良い。

【００３９】具体的な個別情報１５２内のワーク鍵更新開始時刻とワーク鍵更新終了時刻は、それぞれ、例えば、一般的にワーク鍵の更新サイクルは月一回程度と考え、送信予定日時の付加を考慮して、"日"に５ビット、"時刻"を１時間単位の設定として５ビット、合計１０ビットを用いるように構成すれば良い。こうすることで、次回の更新時刻が明確である場合（すなわち加入者の人数の急激な増加や選択する番組の変化がない場合）において、デコーダの電源をより効率的に制御することが可能となる。

【００４０】尚、図３において暗号復号に関する部分（図中破線内）は、セキュリティモジュールと呼ばれ、



最近ではＩＣカード等にアルゴリズム及びワーク鍵KWの記録部分を持たせることで、デコーダ本体と分離する傾向にあるが、この場合においても、個別情報の更新時間情報の更新をＩＣカード（セキュリティモジュール）に記録させることで同様な効果を得ることができる。

【００４１】また、上記実施例では、暗号鍵を３重としたが、４重以上、あるいは１重、２重でもよい。

【００４２】

【発明の効果】以上説明したように本発明の送信装置によれば、暗号鍵と更新情報を伝送するようにしたので、無駄に電力を消費することなく、暗号鍵を確実に更新させることが可能になる。

【００４３】また、本発明の受信装置によれば、暗号鍵を更新毎に書き換えて記憶すると共に、更新情報に基づき電源を制御するので、簡単かつ確実に、暗号鍵を効率的に更新することができるという効果がある。

【図面の簡単な説明】

【図１】本発明の送信装置であるエンコーダの一実施例の要部の構成を示すブロック図である。

【図２】図１のエンコーダに用いられる個別情報の一構成例を説明する説明図である。

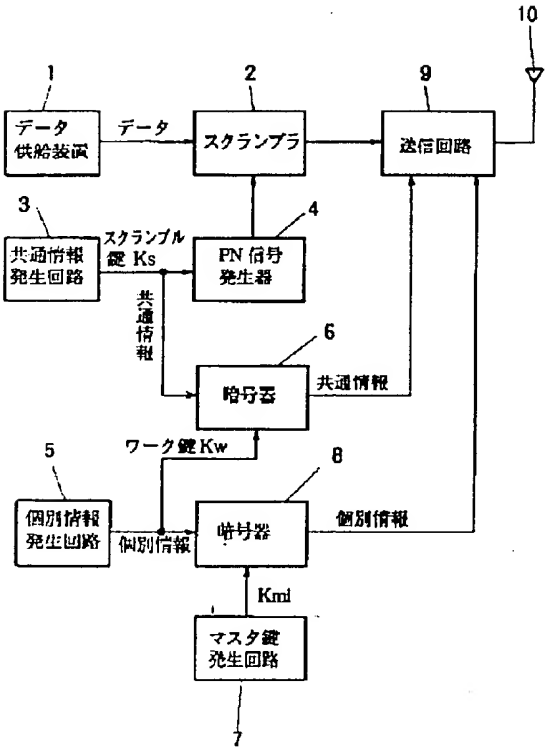
【図３】本発明の受信装置であるデコーダの一実施例の要部の構成を示すブロック図である。

【図４】従来の有料放送の送信装置及び受信装置の構成を示すブロック図である。

【符号の説明】

１　データ供給装置
２　スクランブラ
３　共通情報発生回路
４　ＰＮ信号発生器
５　個別情報発生回路
６　暗号器
７　マスタ鍵発生回路
８　暗号器
１０１　ＢＳチューナ
１０２　パケット分離回路
１０３、１０４　暗号復号器
１０５　記憶部
１０６　デスクランブラ
１０７　ＰＮ信号発生器
１０８　条件比較器
１０９　時間情報記憶部及びタイマ
１２０　サービスデコーダ
１２１　電源制御部
１２５　電源

【図１】

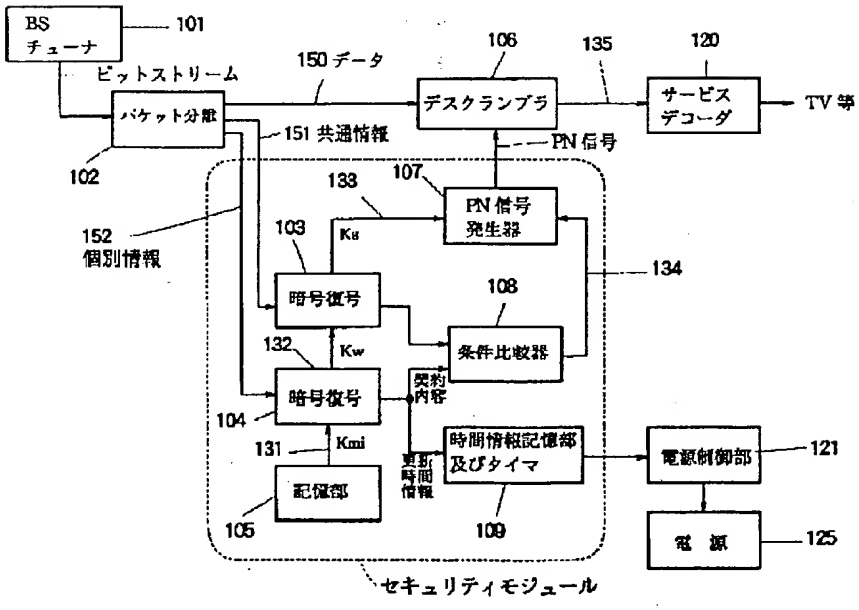



【図２】

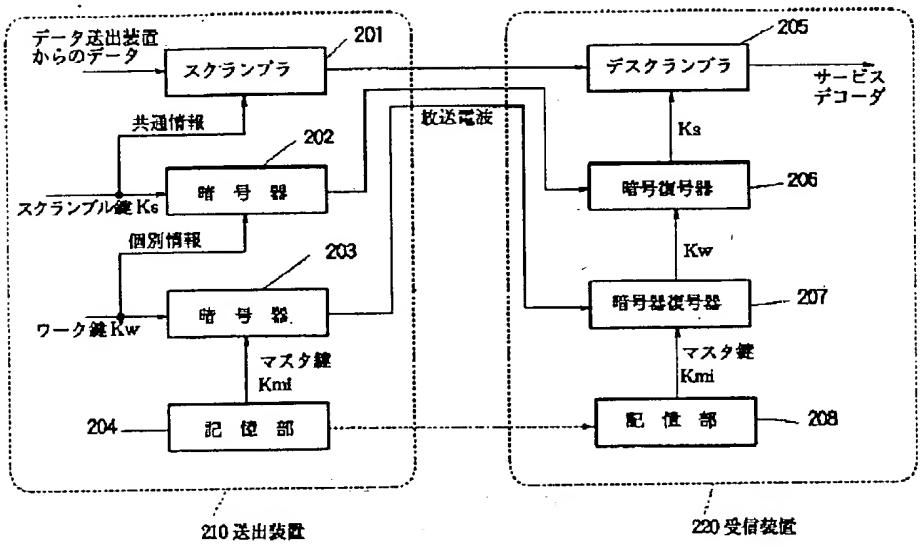
152 個別情報

| | 項　目 | ビット数 |
|---|---|---|
| 161 | 符号化識別 | 16 |
| 162 | 関連情報識別 | 2 |
| 163 | ユーザー ID | 32 |
| 164 | ワーク鍵 | 32 |
| 165 | ワーク鍵対象番組 (PV, SV, PR) | 40 |
| 166 | 契約登録コード | 12 |
| 167 | 鍵有効期限 | 11 |
| 168 | 個別情報送信予定日時 | 10 |
| 169 | 改ざん検出 | 16 |
| 170 | その他 | 5 |

【図３】



【図４】


データ送出装置からのデータ
201
スクランブラ
共通情報
202
暗号器
スクランブル鍵Ks
個別情報
203
暗号器
ワーク鍵Kw
マスタ鍵Kmi
204
記憶部
210送出装置
放送電波
205
デスクランブラ
サービスデコーダ
Ks
206
暗号復号器
Kw
207
暗号器復号器
マスタ鍵Kmi
208
記憶部
220受信装置